The Final Divide of the Economy and its Support System

Vincent Mascarenhas, Ph.D.

Master of Computer Applications (MCA)
St. Aloysius Institute of Management and Information Technology (AIMIT) "WINDHAVEN", Pais Hill Road, Bejai,

Abstract – The purpose of this research is to look into the current looming threat of Cloud Computing and the effects of these services on users in terms of managing their personal information and financial assets. Management teams of companies big and small are responsible for safeguarding the interests of their customers. In the 2007 time-frame when the financial crisis gripped the U.S. economy, the gap between the rich and poor widened further. This was brought on by companies with no accountability whatsoever toward the general public. Cloud services are becoming similar in nature to financial services which owing to weaker control over the growing organizational structures, management and operational issues, would result in mergers and acquisitions. The human sluggishness and greed at the top management level, leads to the problems for majority of the population, honest investors and customers. Cloud Computing could be another catastrophe that needs to be avoided and contained within explicitly defined limits.

Keywords - cloud computing; economy; support; system; data; security; accountability; service provider; cloud service.

I. INTRODUCTION

The fervor of Cloud Computing has permeated every industry and every field of technology. However, the dangers of this aggressive stampede toward Cloud Computing are not well established or researched. Hype of Cloud Computing that has drawn so many of us toward this technology is but a failing on our part rather than an educated enterprise toward better management of information.

Is this the final divide between corporations and their customers, governments and the common man? Cloud Computing will result in an increasing hold on global information by few who then could control the masses by way of controlling the information and in turn, the financial assets.

Porting applications on data analytics to the Cloud is looked at only from a perspective of cutting down the processing cost. Lowering the operational cost of data processing in an organization, even though a flawed rationale is not the only factor or measure that needs evaluation. The focus should be on the long-term effect on how and who will handle, rather control information.

II. DATA LOSS

If a parallel analogy could be drawn between Cloud Computing and the financial crisis of 2007 – 2008, here are some of the areas that are common signifying a need for extensive analysis and research. The impact of the financial crisis that realized is still being felt by everyone and not just the investors and home-owners in the United States, whichever way one justifies the wrongdoing of the mega-corporations. Overnight loss of personal wealth suffered by everyone except the management on higher strata has left thousands impossessed. Code of Ethics in these companies may have been forced down on all employees to be strictly adhered to, but the higher management was not bound by its principles and values. The compensation given to a few if properly administered, could have been used to deflect the full negative impact on the economy but that conscious outreach was devoid of legal traction. In any area, once the damage is done, retraction and backtracking comes across major hurdles as the reprobates are more efficient in using the loopholes in the system.
Information is wealth, and the loss of information or the hold on it by the Cloud service providers will have similar consequences, as in financial losses, if not controlled and confined to its limits.

Customer data is not the property of financial institutions and/or companies that store it. The data they hold and process belong to the consumers and the common man. Once the data are out of certain area of jurisdiction, a characteristic of the

Cloud, the use of that information will be unpredictable and is prone to mishandling and abuse. This may be further compounded by the level of security which will only be as strong as the security that service providers have in place. To this extent, in an overarching impulse, the Cloud service providers have an obligation to protect consumer data. Data access is totally dependent on a company's security system and having proper security controls around data is innately a part of managing a business.

Factors deserving serious consideration before we get deeper into the quick-sand of Cloud Computing are:

- Data spill over
- Data freeze
- Total loss or unavailability of data

III. SELLING POWER

Cloud service providers such as Amazon, Google, Savvis, Verizon and others may have either spare power they need to sell or are hoping to startup virtual environments as Cloud providers. Practical operational issues, if not properly managed, will result in mergers of small service providers later on. The resulting fallout will have to be borne by the common man. As could be seen in the aftermath of the financial crisis, no one entity public or private was able to sort out the problems of the common man and compensate the investors or home-owners. Apart from total lack of genuine responsibility the only outcome of the whole crisis was the blame game that was well played by everyone at fault for this disaster. Once caught in the bureaucratic entanglement these issues only got worse and affected other areas of the social and economic configuration.

IV. CONTROL SPAN

Power and constancy are well defined when a control area is small. The pervasive human nature is to hoard information and intellectual property of all sorts. As the control area of companies broadens and that of the common man narrows down, it is naturally prone to exploitation. With the kind of irresponsibility so deeply ingrained in the social, economic and political systems, the broader the control area, the more insecure is one's personal information. Control issues are fundamental to conflict of interests when it comes to multiple participants and entrepreneurs.

V. VULNERABILITY

Falling in line with the widening and intangible control area is the data vulnerability. Personal information owned by one service provider may in all likelihood go to sub-vendors. There are no laws drawn yet on liability on the part of service providers. If there is no guaranteed or controlled flow of liability information about data transfer between two service providers, it might even mean that the information that is in the hands of the original vendors may end up with some sub-vendors whose installations may be exposed to hacking and viral attacks. Such complicated and obscure agreements and ambiguous contracts drawn by companies are out of the purview of a single investor or the common man.

VI. DATA PRIVACY AND ETHICS

Customer sensitive information is a well-protected asset. Under certain circumstances, it may also be greatly desirable if legal investigations are called for and may even be prone to legal seizure. A question of legal jurisdiction may be a well sought after area for further research.

Organizational growth, efficiency and strategies should all be bound by ethical use of customer sensitive data. Unscrupulous use of customer data for marketing leverage is one of the key areas of customer exposure to risks and losses.

VII. MOORE'S LAW

With the increase in processing speed and processor capacity, the current challenge in the industry is not of data storage but of data retrieval. There is dramatic decline in the prices of hardware, the upshot of which is that the data stored is more voluminous and may even be redundant and sometimes be irretrievable. Companies may slice, dice, analyze and index billions of records into petabytes of data. This is not because of unavailability of storage space, but because of their need to get the full essence as business intelligence from what has been stored – tactical and strategic.

Efficiency of retrieving relevant data at the right time is a challenging task. Big Data is an issue that needs to be dealt with by way of improving data retrieval efficiency techniques. Current technological innovations are leaning more toward solving the problem of efficient data retrieval rather than storing it. We are now operating in reverse mode, that is, more data requiring lesser space. The cost of storage devices is cheaper and the value of information is greater.

VIII. DATA SECURITY

Data security is as abstract a subject as that of Cloud Computing. Privacy laws will have to be reviewed, streamlined and simplified. Information held to ransom by the service providers could be a major issue of using the Cloud. The major part of the problem in the Cloud is security which is more of a hands on issue than a talked about hype. Computer security has always been number one in terms of priorities. A company that is known to have computer installations within could manage security issues better compared to an entity dealing with security that is not within its realm of control. A radical departure from internal security mechanism to an external up-in-the-air security is not a good blessing for the management and even more for the clientele. In unexpected bankruptcies eventually the companies will transfer the data to other service providers. Irrespective of whether there are security issues or compatibility issues, the idea itself is not very comforting. Companies that use Cloud services will be transferring the rising cost from one side of the balance sheet to the other and still have no control over their data.

IX. BACK-UP PLAN AND NETWORK FAILURE

Companies have systems to fall back on at any time a crisis arises. A back-up plan for systems is not given much importance by supporters of Cloud Computing. Even though virtualization is a norm and the advocates talk much about it, when the real disaster strikes it is the clients or the owners of data that are left to fend for themselves. Some of the biggest banks currently operating in the U.S. use legacy systems and function 24/7 on back-up systems. In these cases, instantaneous mirroring of every single transaction, financial and non-financial, from the production server to the back-up server is essential for the uninterrupted functioning of the 24/7 system availability. System downtime is a thing of the past. Considering the overheads and unknown hitches, a successful recovery from a back-up site can be challenging while operating on the Cloud.

Apart from the compatibility issues, one of the key areas we need to focus on at the time of data recovery is the band-width. Data recovery coupled with a collapse of networks could be a major disaster area for users of the Cloud. The restoration of data from the Cloud back-up could at times be counter-productive if there isn't a well-tested recovery plan in place having considered all issues as to what is required or rather critical to business and what is not.

Major disasters in the past are known for unpreparedness on the part of the management. Apart from human complacency a typical failure of a production service is the unexpected nature of disasters. The difficulties inherent in applying the use of Cloud service to the operational workflow will further deteriorate business performance.

X. THE ELUSIVE CONROL

If Cloud service providers go bankrupt, who will own our data? People invest in different financial sectors and in current environment, financial institutions to a certain extent are held ethically liable for these investments.

Though accountability is never voluntary, there always has been a physical or tangible control of the set up for the customers. The more intangible an entity having control over the data the more uncertain we are about taking it seriously. Problem of vendor accessibility is another factor that needs extensive research.

XI. MUTE ANALOGY

Similarities have been drawn between Cloud Computing and utilities such as water and electricity but these analogies do not hold any water. When these essential utilities fail, it is one local unit that fails, big or small that is affected and the localized clout works toward solving a common problem. It is contained within certain geographical limits and is within the confines or sphere of certain authorities.

We cannot personalize the contents of electricity and water. Personal information is not comparable and be considered equivalent to these natural resources. Water and electricity cannot be termed as customer sensitive as we consider the sensitive nature of our personal data.

There is a huge difference between these utilities and Cloud services. There are other sources that provide electricity and water but personal information that is inaccessible cannot be acquired from other sources.

XII. ACCOUNTABILITY

A lot has been seen and sensed about this so called accountability. If we take into consideration the past experiences in the financial sector, we as consumers are aware how much of this sense of ownership has been seriously acknowledged by the companies and service providers. If not for their total disregard, the economic frontier would have been less subdued. Accountability is totally lacking in the current environment of any business. Promise of service is as good as the first installment paid to a company. Once the customer is lured in with all kinds of attractive offers, the real concerns surface at the time the consumer is actively using the product or the service.

XIII. STANDARDIZATION

Desirability, rather the appeal of standardization from communication protocols to browsers to video streaming is an idea that is supreme in its all-deserving halo. Everywhere there is talk about standardization but in our daily life we see issues related to incompatibility and hundreds of software versions of different kinds put a heavy burden on the common user. Standardization issues could be unintentional but are long lasting.

Deviation from standardization by companies could be, among other strategies, to beat down rival businesses. This could be one of the major areas of concern while considering the compatible nature of Cloud services in driving an efficient business venture.

XIV. VENDOR INVISIBILITY

Startup Cloud service providers especially are a major threat to Cloud Computing. These companies need to have well regulated and monitored systems to host these services. If 20/20 hindsight has taught us well or not, there has been total contempt and impertinence on the part of the companies providing any kind of service.

	RISK		OPERATIONAL COST		DATA VULNERABILITY		FINANCIAL/ PERSONAL LOSS	
	Owned By		Owned By		Owned By		Owned By	
Category	Consumer	Cloud	Consumer	Cloud	Consumer	Cloud	Consumer	Cloud
Virtualization of Systems	N/A	N/A	Minimal	N/A	N/A	High	N/A	N/A
Computing as Utility	None	None	Minimal	N/A	N/A	High	None	None
Software as a Service	N/A	N/A	High	Minimal	High	High	None	High
Service Fee	High	High	High	Minimal	Minimal	High	Minimal	High
Data Security	Minimal	High	High	High	Minimal	High	High	High
Data Privacy	High	High	High	High	None	High	High	High
Data Value	High	High	High	High	None	High	High	High

TABLE I. DATA RISK FACTOR FROM MINIMAL TO HIGH

First, extremely stringent laws should be established. Cloud service providers should shoulder the entire financial responsibility for any misuse or loss of data. Each individual might have a different vendor or a service provider. The problem with a failed service is that the time taken to fix the problems is dictated by the service level agreements drawn out by the companies providing the service which may not be in line with the critical business needs of the consumer that is dependent on it for its data. It is always difficult to contact the vendors at the time of need. The elusive control of sensitive data will be given to some elusive vendor somewhere and this may be an added burden for the consumer.

Even major banks have had down-time issues that were not in their control. As the emerging service providers are wholly dependent on other factors such as communication lines the availability of system however critical to the consumers is subject to delays and inconsistent service. There is too much of inter-dependency of different areas of communication network related components that needs to be looked into for a smooth functioning of a business unit.

To site good examples of what could go on the Cloud are bookshelves and information archives like the encyclopedia or government agencies that provide Cloud services to the public. Banks and financial institutions should not go on Cloud for the simple reason that it holds sensitive information of the general public. Consumers take all precautions to safeguard personal information but if the same information is provided to the financial institutions in an obligatory act and if that information is misused or mishandled, it is not an acceptable or a justifiable act. What is more important for any individual is his or her economic and social worth. Once those are compromised, the general public do not have control over them and the legal entities will never be able to deliver a solution in time.

XV. THE THREAT

The threat of Cloud Computing is overtaking us just like the significance of the term "Cloud". It is clouding our minds with a wrong notion by giving the users and the Cloud advocates a wrong sense of exhilarating feeling of this new technology. It could be used to a certain extent, but should take into consideration the risks. Unavailability of critical information, compromised security and loss of control of one's own information could be major issues and these need to be addressed by all Cloud operators and service providers.

XVI. RESOLUTION

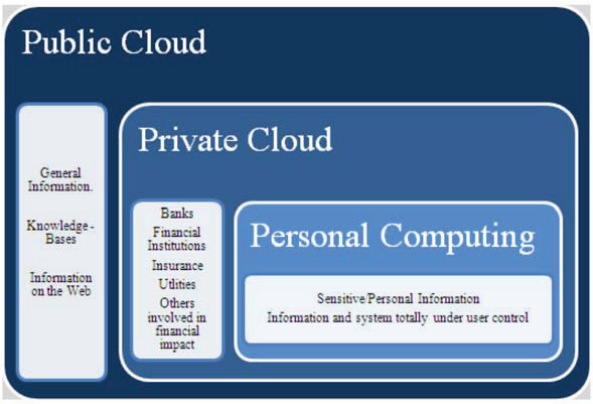

Figure 1. Data Boundaries in the Cloud – What may or may not go on a Cloud

A. Personal Computing: Non-Public Information should be completely within the control of a user. Any information that is critical, time-sensitive or private should be kept away from the Cloud.

B. Private Cloud: Organizations should limit to Private Clouds to safeguard the customer sensitive information such as:

- Customer information (Non-Public Information)
- All types of customer transactions
- All kinds of customer profile gathered at the time of transactions
- Customer correspondence
- Customer banking information
- Any other information that could be used against a customer

Companies currently do store customer information for operational use and statistical data for applications like Customer Relationship Management (CRM), Business Intelligence (BI) and Enterprise Resource Planning (ERP). This information should never get into Public Cloud. Strict regulations should be enforced to confine this information to Internal or Corporate Clouds.

C. Public Cloud: General public information that is not proprietary, time-sensitive or customer sensitive such as the following can go on Public Cloud:

- iPhone iTunes, music, videos and other information which is equivalent in nature and value.
- Knowledge-Bases and sources of information such as Blogs, Twitter, Facebook, YouTube, which under the circumstances of any threat do not jeopardize financial or personal security of an individual.
- Information such as contained in public library could be safely stored on Public Clouds.
- Unavailability of a Cloud service should not have a negative impact on an individual's economic and social well-being.

REFERENCES:

[1] Andrew Ross Sorkin 2009 – 2010 - Too Big to Fail.

[2] AnthonyT. Velte, Toby J. Velte, Robert Elsenpeter 2010 – 2011. Cloud Computing – A Practical Approach.

[3] Barry Sosinsky 2011 - Cloud Computing Bible 2011

[4] Kidwell, Blackwell, Whidbee, Sias - Financial Institutions, Markets & Money 2012

[5] John Rhoton - Cloud Computing Explained 2009 - 2011

[6] Vic (J.R.) Winkler - Securing the Cloud 2011

[7] Joel Brenner - America the Vulnerable 2011

[8] Lori Andrews - Social Networks and the Death of Privacy 2011

[9] Lawrence Lessig - Code and Other Laws of Cyberspace 1999